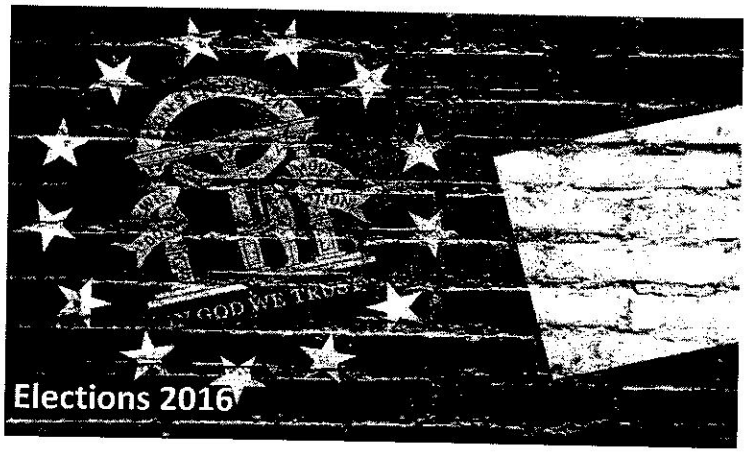


Election Update

August 23, 2016

Helping to Explain Election Security to Your Voters

Election security and integrity is a hot topic in the news. Hacks of the DNC, NSA, and other agencies, online Youtube videos, comments from candidates, news stories, and even suggestions from talk radio hosts have people concerned about the security of our voting system.

Our office, in conjunction with KSU has provided the following points to consider when talking about the security features of our election system. While we can't address every situation or scenario, the points illustrate some basic security features inherent in our system. Keep in mind, however, that YOU and your staff are the best line of defense against attempted encroachment into our voting system. If you review and diligently follow the requirements of the election code and the State Election Board Rules, you will largely prevent opportunities for questions about security to even be considered.

You can always contact our office with specific questions if you have them, and KSU is available to help with questions or concerns about the system and equipment.

Tips for Explaining Security of Election System

1. There is no network connectivity used with any component of the voting system (as you know GEMS can never be connected to any network, the DREs have no wireless or wired connectivity, and the electronic pollbooks are not connected to the Internet.
2. There are explicit rules governing the physical security of the machines (chained together, sealed, kept under lock and key, oaths given to handlers, chain of custody documents, etc.) These requirements prevent unauthorized access to the voting equipment.
3. There is paper documentation of records that could be checked to show discrepancies of total numbers of votes (if a polling place had 250 completed voter certificates, but 600 votes cast on DREs, someone could easily tell.)
4. The GEMS system is very *tamper-evident* if someone accesses the system or tries to inject something into the system, they will leave evidence that they were there. Access to GEMS server is controlled and the GEMS server is locked at all times when not in use. Password protection is implemented at both the operating system and application software level.
5. The sending of the results via the web to ENR does go over the web, but only after the data has been separated from the GEMS server by an "air gap" – that is, data is extracted from GEMS via a secure USB

drive and physically moved to a different computer for upload. Furthermore, ENR data is always checked against GEMS data, so any intercepting or manipulation in transit would be instantly obvious.

6. The units have to be tested publically (Logic and Accuracy Testing) to demonstrate they are working properly before any voting. All such testing has to be documented.
7. As we have a uniform voting system, any discrepancies would tend to be more obvious, and we only have to safeguard and monitor a single system and process. Security best practices are identified and implemented in all 159 counties.
8. All Georgia election officials are required to be certified in the use of the voting system. This training includes 24 hours of training in the use, maintenance and security of the voting system.
9. Voter access cards do not contain any personal voter information. The card contains a code that ensures that the ballot to which the voter is entitled to vote is displayed on the DRE, and a counter that is set to "1" when the card is issued to the voter, and reset to "0" once the voter casts their ballot. Voters can only cast one ballot when issued a card.
10. The GEMS server and its memory cards use SSL encryption to ensure that only those cards created on a specific GEMS server can be used on election night for uploading. An election official cannot close out the election until all of the cards that were issued during the preparation of the election are returned on election night. Any counterfeit cards would be detected and rejected.
11. The DREs require supervisor-level access for all functions except voting. Supervisor cards and passwords are tightly controlled.

OFFICIAL ELECTION INFORMATION

August 30, 2016

TO: All County Election Superintendents, Chief Registrars, and County Election Directors

FROM: Chris Harvey, Elections Division Director

RE: Cyber Security Best Practices

Security is a higher than usual priority for voters this election year. We have outlined below Cyber Security Best Practices to help ensure access to ENET and GVRS is restricted to only authorized users.

- Passwords should not be written down and placed near a workstation.
- Passwords should be at least 8 characters long and utilize capital and lowercase letters, numbers, and special characters.
- Passwords should be changed at least every sixty (60) days.
- Everyone should log out of or shutdown workstations when not in use.
- Workstations should be in a locked environment overnight.
- County Administrators should be aware of all persons that have a key access to areas where workstations, DRE units, and the GEMS server are located.
- When a user no longer requires access to GVRS or ENET, the County Administrator responsible for the user should immediately remove the user's access.
- Avoid accessing GVRS and ENET over unsecured WiFi connections.
- County Administrators should keep an up-to-date list of the access level to ENET granted to each authorized user.
- County Administrators should periodically review ENET usage and passwords to ensure these best practices are being followed.
- Strictly adhere to the data confidentiality provisions of O.C.G.A. § 21-2-225.
- Strictly adhere to the physical DRE units and GEMS server security provisions of SEB Rule 183-1-12.

OFFICIAL ELECTION BULLETIN

September 12, 2016

TO: **County Election Officials**

FROM: **Chris Harvey, Elections Division Director**

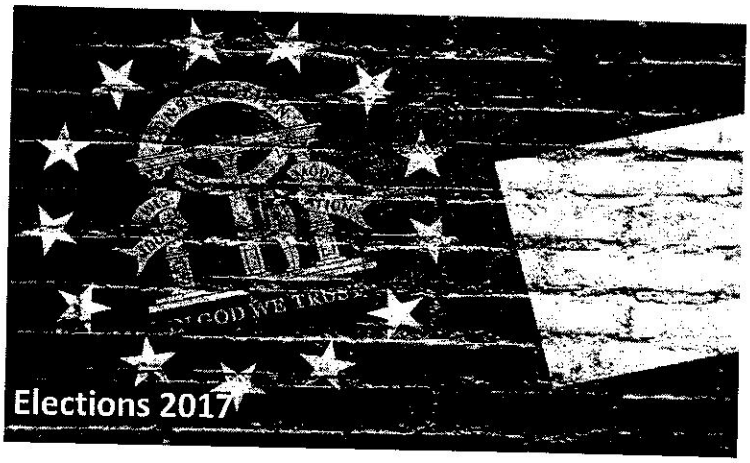
RE: **GEMS Servers and Security**

In light of recent reports regarding election system security and vulnerabilities throughout the country, it is critically important that all counties preserve the security and integrity of their GEMS Server. We have previously sent updates and messages encouraging all counties to be vigilant in following existing requirements for the physical security of all election equipment, including GEMS, DREs, ExpressPolls, and other associated equipment.

With information and advice coming from many sources, it is critically important that every county remember that there should be no program, no product, no update, nor anything else added to or introduced to your GEMS Server without the direct and explicit direction of the Secretary of State's Office and/or Kennesaw State University's Center for Elections. This prohibition includes offerings, products, or solutions from local, state, or federal agencies who may be trying to provide what they feel to be assistance. Whether these solutions are described as "cyber hygiene", "virus protection" or other solutions, these programs simply cannot be introduced or added to your GEMS Server without the direct authorization of the Secretary of State or KSU.

Should any need to take any action with any election equipment arise, you will be specifically and directly contacted by the Secretary of State's Office regarding any such actions. If you ever question any communication from our office as genuine, please contact our office directly.

Again, nothing should be added to the GEMS Server without the explicit and direct instruction of the Secretary of State or KSU.



Election Update

November 3, 2017

Important Security Updates

The security and integrity of the voter registration system and voting system cannot be taken too seriously. The purpose of this Election Update is to provide additional information as well as reminders of previously provided information that will help each election and registration office protect their systems and data from interference, intrusion, or theft.

Kaspersky Software

The Georgia Technology Authority (GTA) just released a letter in which they recommend that all state agencies stop using Kaspersky software immediately. Kaspersky is most commonly found in anti-virus software in computer systems. The Secretary of State's Office is recommending that county and city election and registration offices also stop using Kaspersky software. The full text of the letter from the GTA is below:

"There have been a number of news reports in recent months regarding the security of Kaspersky Antivirus Software. These reports indicate that the federal government is continuing to investigate the product and has instructed federal agencies to develop and implement plans to discontinue present and future use of Kaspersky software and remove those products from federal information systems. Further, the United States Senate passed an amendment to an annual defense policy spending bill seeking to codify and expand the decision to ban the software for use by federal agencies.
Out of an abundance of caution, DOAS and GTA have agreed to restrict the purchase of Kaspersky software as a technology solution for the State of Georgia at this time. Accordingly, it will be removed from Team Georgia Marketplace until further notice.
It is highly recommended that all State of Georgia agencies, departments, universities and colleges identify any current use or presence of Kaspersky software products on their information systems. Agencies currently using those products are strongly encouraged to seek alternatives."

I encourage you all to work with your local IT Departments to ensure that all systems are maintained and protected at the highest possible level. If you are unsure where to seek assistance, please do not hesitate to contact our office, and we will help you find help.

Phishing

"Phishing" is a term that refers to various attempts to get information through email. Other similar terms are "spearphishing" and "spoofing," but they are variations on a common theme. A common way to be victimized is to receive an email that appears to be from a legitimate source and asks for

some information from the recipient. Sometimes the request is for a username and password, PIN, or some other confidential information. In other cases, the "phishing" email will contain a link that you can click. In some cases clicking on the link will install malware or other destructive programs on the recipient's computer. In some of these "phishing emails" graphics such as headers and emblems may be carefully copied on the email to better gain the confidence of the recipient.

Yesterday, I became aware that several election officials received an email that had my name and email address attached to it, making it appear as if the email came from me. The email contained verbiage about payment and a bank and additionally contained a link to an unknown web address. Our office responded with our cyber security team and ultimately concluded that the email was a "spoof" email using my name and email address only (the email did not originate in our office or pass through our servers). This is a timely reminder that everyone should handle *all* electronic communications with care and discretion, and to confirm or further investigate anything that seems out of the ordinary (such as the Elections Office sending you an email about a payment.)

Know that the Secretary of State's Office will NEVER email you and ask you to provide sensitive information such as passwords, PINs, or other similar data. Likewise, we avoid sending hyperlinks to you via email without personally notifying you in advance. Should you receive a suspicious email or other contact from our office, please contact our office directly by telephone before responding to the suspicious contact/email or clicking on links or attachments.

Specific Email Phishing Incident

The following alert is one we received from Department of Homeland Security. This did NOT happen in Georgia, but the memo describes an incident that, involved an email appearing to be from the Election Assistance Commission (EAC) that would have been of particular interest to election officials.

A state elections agency received a malicious spam email that impersonated (spoofed) an employee of the U.S. Election Assistance Commission (EAC) and links to a malicious URL that attempts to download malware. The Multi-State Information Sharing and Analysis Center (MS-ISAC) believes the malicious spam email was part of a national campaign to disseminate Emotet malware. Emotet is a Trojan that is known to download other malware and once it compromises an account, emails itself to all the contacts in a victim's address book. Since April 2017, Emotet has used the names of varying agencies, including the MS-ISAC and the U.S. Department of Homeland Security (DHS), in its malicious spam campaigns.

Emotet is financially-motivated and in recent months has been one of the most prolific pieces of malware in the state, local, tribal, and territorial government domain. The malicious actors behind Emotet seek to make a profit by downloading other malware onto infected systems or using system resources for other purposes. The dropped malware has included Pinkslipbot, Dridex, and Corebot/Trickbot, which makes a profit through similar techniques, such as collecting financial information or forming a botnet to conduct malicious activity for a fee. Historically, as a Trojan, the Emotet malware has used Word documents or PDF files to trick users into downloading/opening what the user believes are safe files. These files are infected with malicious code that then downloads Emotet. In this current campaign, when the user receives the malicious spam email, the email directs the user to click on a link. The link reaches out to a malicious URL, which then facilitates downloading Emotet.

Part of Emotet is a scraper module that gathers names and email addresses from a victim's Outlook account and uses that information to send additional emails. The malicious actors behind the Emotet campaign use this as a social engineering technique, since a victim's contacts are likely to respond to a similar email as the victim did. Thus by using the name of a reputable agency and impersonating a trusted contact, the malicious actors ensure the wide distribution of malicious spam emails to a relevant audience.

Emotet also contains a network enumeration module. This module involves a self-extracting compressed file containing two components, a bypass and a service component. The bypass component is used to identify network resources, such as share drives with write access, and tries to gain access to user accounts, such as the administrator account, by using brute force techniques. Once an available system is found, Emotet then uses the service component on the system to install itself.

If you receive an email that appears unlike normal EAC communications or an email appearing to originate from a contact, that is unlike normal communications from that contact, it may be a part of this malicious spam campaign. Your information technology (IT) department or the MS-ISAC can assist you in determining whether or not the email, link, or attachment should be trusted. Requests for these services can be obtained by calling 1-866-787-4722, replying to this email, or sending an email to SOC@msisac.org.

Recommendations

We recommend the following general best practices, to limit the effect of malicious emails and scams on your organization:

- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
- Recently, Emotet has been able to bypass email security filters, so the MS-ISAC recommends educating end users about spam and social engineering tactics. Remind them never to click on links or open attachments delivered with unusual, unexpected, or unsolicited emails.
- If you don't have a policy regarding suspicious emails, consider creating one and specifying that all suspicious emails should be reported to the security and/or IT departments.
- Use antivirus programs on clients and servers, with automatic updates of signatures and software.
- Implement filters at the email gateway to filter out emails with known phishing indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- Utilize Sender Policy Framework (SPF), a validation system that minimizes spam emails by detecting email spoofing and allowing administrators to specify who is allowed to send email from a given domain by creating a SPF record in the Domain Name System (DNS).
- Adhere to the principal of least privilege, ensuring that users have the minimum level of access they need to accomplish their duties.
- Adhere to best practices, such as those described in the CIS Controls, which are part of the CIS SecureSuite.

If a user opened a malicious email, we recommend:

- Run an antivirus scan on the system and take action based on the results to isolate the infected computer and reimage it.
- If an infection is found:
    - users should change their passwords to any account accessed on the infected system; and
    - review the Outlook mailbox rules associated with the user account to ensure further compromises have not occurred, including the creation of an automatic rule to autoforward all emails to an external email address.

GEMS Must Remain Permanently and Completely Offline

Everyone should know that the GEMS Server must be remain "offline" at all times. The GEMS Server must never be connected to a network. Additionally, no other software, other than what is already provided by the Secretary of State's Office through KSU can be added to any GEMS Server. Election officials must remain vigilant custodians of their GEMS Servers.

ENET Security Enhancements

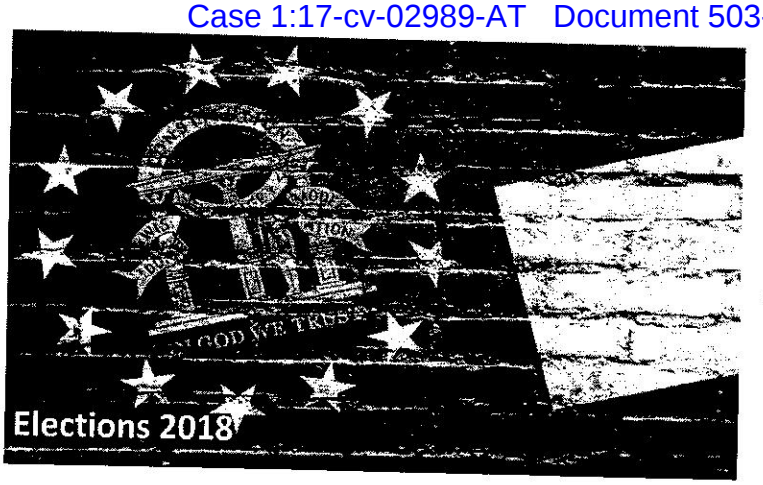
We have added expiring passwords, odd-hour ENET alerts, anti "brute force" password defenses, and user audits to enhance ENET security. We are working on additional security features to continue to secure ENET, and will share these features once they are in place.

Physical Security

Remember that physical security of election equipment (DREs, ExpressPolls, memory cards, keys, etc.) is a major component of election security. The details of storage and security can be found in the State Election Board Rules in sections 183-1-12-.02(2) and following. All care must be taken to ensure the physical security of the voting equipment. Careful documentation of the tamper-evident safeguards such as the numbered seals on secured devices before, during, and after elections provide real security and enhance voter confidence in the security of our system.

Keep Vigilant

Investigations have shown that even the most effective cyber-security measures cannot protect systems from human errors. In many cases, these errors are errors in judgment regarding clicking on an attachment or link in an email, or responding to a pop-up message on a website asking for protected information such as a password or username. When in doubt, ask a question or confirm that something is authentic. If something doesn't seem right, safely investigate or ask for help.



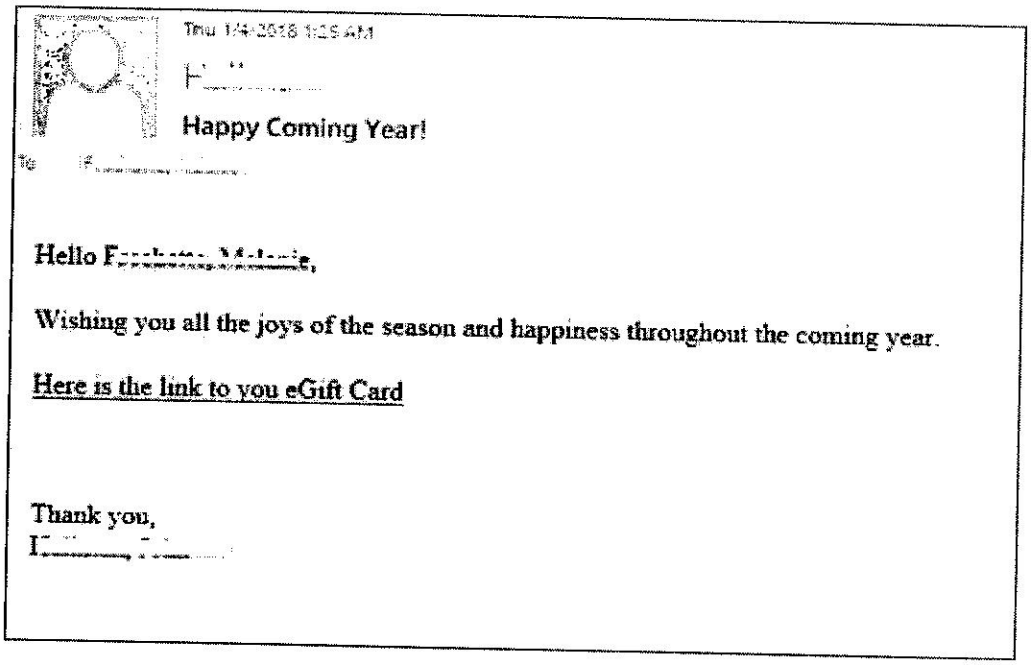
Election Update

January 5, 2018

More Email Phishing Information

Email "Phishing" schemes are becoming more common, and I want to make sure everyone is aware of best practices and cautions in dealing with "Phishing" emails.

A "Phishing" email is usually an email that appears to be from a legitimate or known source, and usually contains a link or attachment that the recipient is encouraged to click on or open.



Thu 1/4/2018 1:25 AM

Happy Coming Year!

Hello [redacted],

Wishing you all the joys of the season and happiness throughout the coming year.

Here is the link to you eGift Card

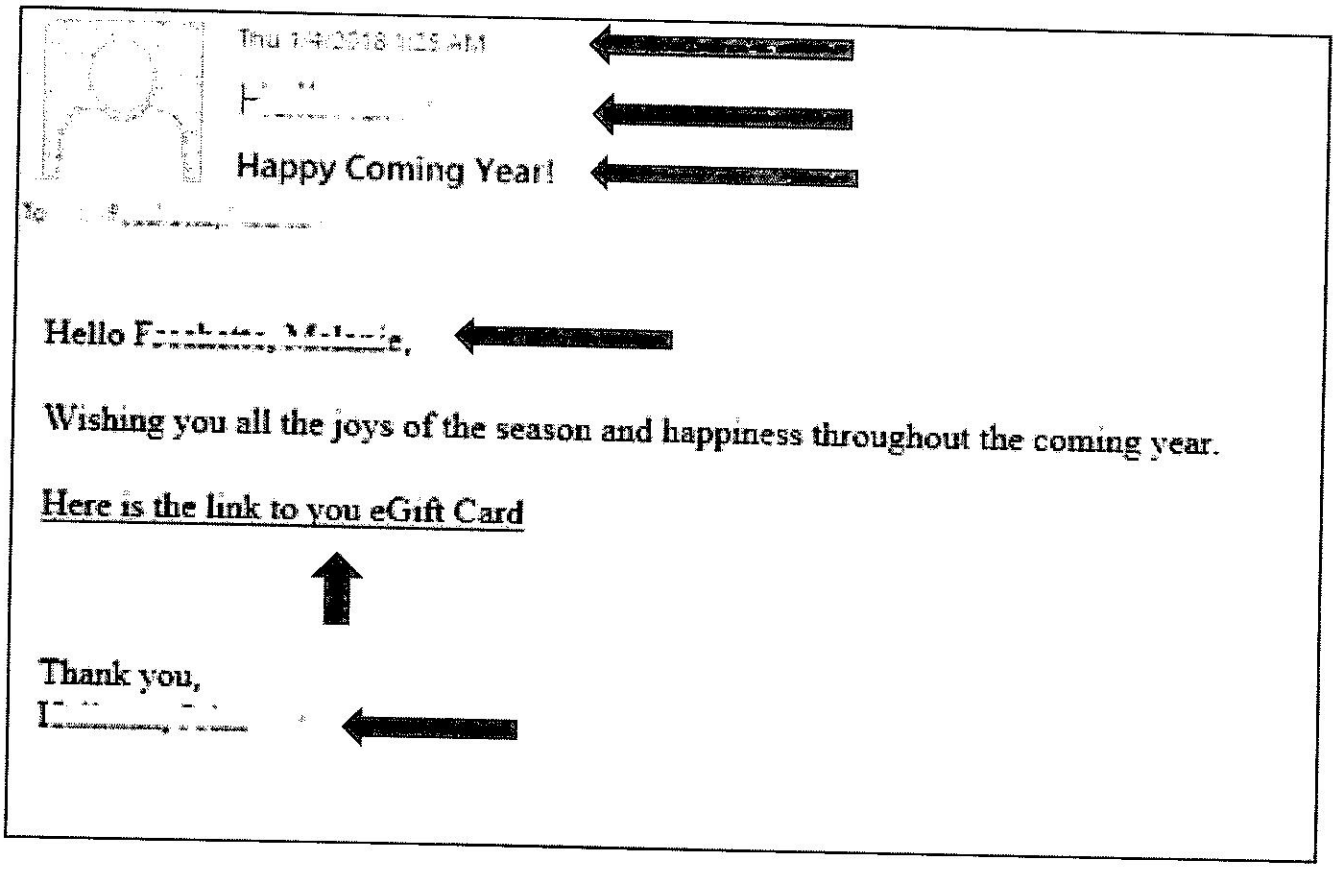
Thank you,
[redacted]

Opening attachments or clicking on links can cause viruses or malware to be installed on your computer which can include a "keystroke log" which may capture all usernames and passwords.

CHRIS HARVEY | ELECTIONS DIRECTOR | SECRETARY OF STATE'S OFFICE | (404) 656-2871

Let's look at that email again and notice a few oddities that should catch the eye of the recipient.

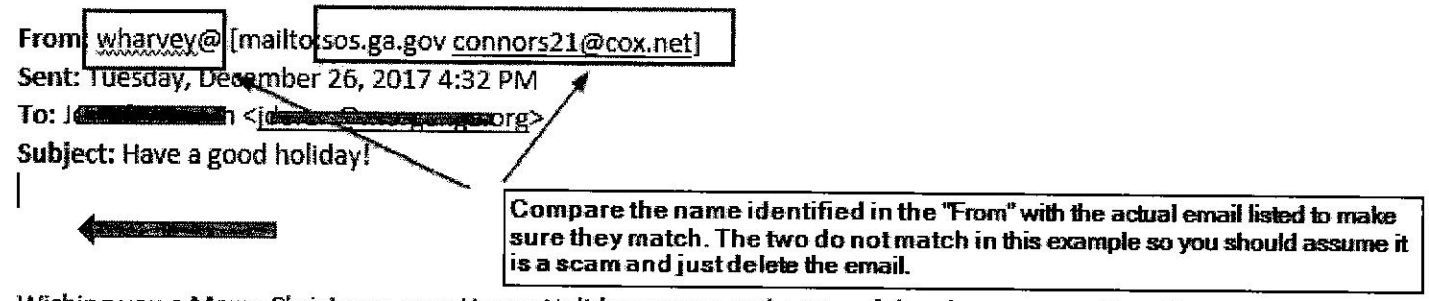
This email was received by a person who knows and works with the purported "sender."



The Arrow Directory

1. The email was sent at 1:25 AM. Not typical working hours.
2. The Last Name (only) of the sender was listed.
3. "Happy Coming Year" isn't typical language used by most people.
4. The greeting lists the last name, first name, which is hardly typical for a friendly email.
5. Grammatical error "you eGift Card" when the proper grammar is "your eGift Card"). Also, an unusual gift, out of the blue, seems a little too good to be true.
6. The signature line list the "sender's" last name, first name, which, again, isn't customary in a personal email.

Let's look at another apparent Phishing email that was received by a county official.



Wishing you a Merry Christmas, very Happy Holiday season and a peaceful and prosperous New Year.

Here is your gift card

Warmest Regards,

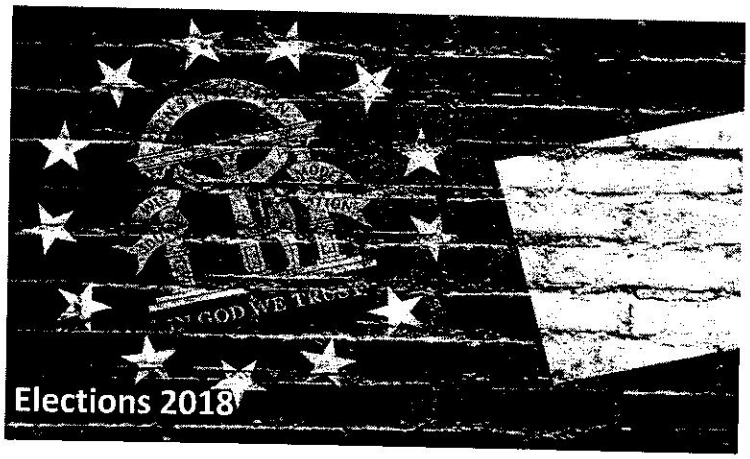
wharvey@sos.ga.gov

Georgia Open Records Act: Under Georgia law, all information, including e-mail, written letters, documents and phone mes Commissioners and County offices and employees is subject to Public Records law. This includes the sender's e-mail addres shown in the message, the content of the message and any associated attachments to the mail.

1. The name on the sender did not match the email address from which the email originated.
2. There is no personal salutation.
3. The signature is a link/email address.
4. The email is an unexpected and unannounced "gift."

Some "phishing" attempts will be better than others. When in doubt, initiate a new contact with the sender to confirm that the email is genuine. If you cannot confirm the authenticity of the email, consider deleting it.

As always, our office will be happy to confirm anything that comes from us if you have questions about authenticity.



Election Update

February 21, 2018

OPEN RECORDS REQUESTS FOR ELECTION DATA FILES

Election Officials,

Some of you may have recently received Open Records Requests from the Coalition for Good Governance and/or Marilyn Marks requesting copies of DRE memory cards and ExpressPoll memory cards. This Election Update is to make clear our office's expectation on how to handle those requests. Marilyn Marks is the Executive Director of the Coalition for Good Governance, a group that has sued Georgia alleging that the election machines currently utilized are not secure and asking a judge to order the state not be allowed to use them in the upcoming elections. This is a serious and false allegation. That litigation is ongoing.

Our office has discussed the requests with our technical experts and with the Georgia Attorney General's office. **Under no circumstances should a copy of original election data files from DRE memory cards or ExpressPoll memory cards be provided to unauthorized third parties, including through an open records request.** A full copy of either the DRE memory card or the ExpressPoll memory card may reveal the architecture of the database and how data interacts within the voting system and are exempt from the Georgia Open Records Act pursuant to O.C.G.A. § 50-18-72(a)(25(A)(iv). The Georgia Court of Appeals has cited this provision in upholding an injunction against a county proposing to release sensitive election data. That case, Smith v. Dekalb County, 288 Ga. App. 574 (2007), is attached to this update.

If you plan to send out this information despite this warning, please let our office know immediately so that we might take appropriate action.

Please keep in mind that there is some data on the DRE memory cards or ExpressPoll memory cards that could be considered public records, but our office and county election officials must be extremely sensitive to the format that information is in if released so that sensitive information is not able to be attained along with public information. We will be happy to work with you and your county attorneys on identifying what information could be released and how to do so in a safe way.

Please let us know (as well as your county attorney) if you receive an open records request that involves DRE memory cards or ExpressPoll memory cards. Remember that you have a duty to respond to record requests you receive, but the Open Records Act does not in any way require you to endanger the security of Georgia's election system. Georgia's election system remains secure due in no small measure to the work that your offices do to limit access to voting machines and sensitive data to appropriate personnel. Now more than ever we must stay vigilant to keep our voting system secure.

CHRIS HARVEY | ELECTIONS DIRECTOR | SECRETARY OF STATE'S OFFICE | (404) 656-2871

Smith v. DeKalb County

Court of Appeals of Georgia

November 27, 2007, Decided

A07A1490.

Reporter
288 Ga. App. 574; 654 S.E.2d 469; 2007 Ga. App. LEXIS 1254; 2007 Fulton County D. Rep. 3715

SMITH v. DEKALB COUNTY et al.

Subsequent History: Cert. applied for.

Writ of certiorari denied *Smith v. DeKalb Cty., 2008 Ga. LEXIS 291 (Ga., Mar. 10, 2008)*

Prior History: *Open Records Act*. DeKalb Superior Court. Before Judge McMurray, Senior Judge.

Disposition: **[***1]** Judgment affirmed.

Core Terms

election, records, ballot, permanent injunction, superior court, trial court, inspection, software, seal, exempted, designated, encryption, returns, voting, codes

Case Summary

Procedural Posture

After a requestor sought election documents under the Georgia Open Records Act, *O.C.G.A. § 50-18-70 et seq.*, the Georgia Secretary of State sought a permanent injunction preventing a county from releasing a certain computer disk - read only memory (CD-ROM). The DeKalb County Superior Court (Georgia) enjoined the county from releasing the CD-ROM. The requestor appealed.

Overview

The court first stated that the trial court properly held that the Secretary had standing to object to the request. Under *O.C.G.A. §§ 21-2-30*, *21-2-31*, *21-2-32*, *21-2-50 et seq.*, and *45-13-20 et seq.*, the Secretary was charged with the supervision of all elections in Georgia. Next, under *O.C.G.A. § 21-2-500(a)*, the custodian of a CD-ROM created by an election superintendent had to maintain it under seal following the election for at least 24 months, unless otherwise directed by a superior court. A superior court had not ordered that the seal be lifted. Thus, the CD-ROM was by law prohibited or specifically exempted from being open to inspection by the general public under *O.C.G.A. § 50-18-70(b)*. Furthermore, the trial court had found that release of the CD-ROM, which contained passwords, encryption codes, and other security information, would compromise election security and thus was exempt from disclosure under *O.C.G.A. § 50-18-72(a)(15)(A)(iv)*. Although the requestor argued that the State could copy the CD-ROM without including such information, *O.C.G.A. § 50-18-70(d)* provided that an agency was not required to create records that were not in existence at the time of the request.

Outcome

The court affirmed the judgment.

Counsel: *J. M. Raffauf*, for appellant.

Thurbert E. Baker, Attorney General, Stefan E. Ritter, Calandra A. Almond, Assistant Attorneys General, William J. Linkous III, for appellees.

Judges: ELLINGTON, Judge. Andrews, P. J., and Adams, J., concur.

Opinion by: ELLINGTON

Opinion

[*574] **[**469]** ELLINGTON, Judge.

Philip Smith appeals from an order of the DeKalb County Superior Court granting a permanent injunction to Cathy Cox, in her **[**470]** official capacity as Georgia's Secretary of State. [1] Smith contends that the

[1] Cox's term as Georgia's Secretary of State has since

court erred in finding that the Secretary of State had standing to pursue the injunction, in granting the Secretary of State's request for temporary restraining orders and the permanent injunction, and in denying his motion to recuse. For the following reasons, we affirm.

The record shows the following facts. On October 23, 2006, Smith's attorney, Mike Raffauf, submitted a written request, pursuant to the Georgia *Open Records Act*, *OCGA § 50-18-70 et seq.*, to Linda Latimore, the DeKalb County Director of Voter Registration and Elections, for disclosure of certain information concerning the 4th Congressional District 2006 primary and runoff elections. Raffauf requested that Latimore make available for copying and inspection the following materials:

> A copy of the GEMS CD-ROM(S), **[***2]** [2] generated pursuant to *OCGA § 21-2-500 (a)* [3] and [Rule of the State Election Board] **[*575]** 183-1-12-.02 (6) (a), [4] which contains a copy of the information on each memory card (PCMCIA Card) which shall include all ballot images and ballot styles as well as vote totals and a copy of the consolidated returns from the election management system.

According to Raffauf's request, "[a] review of the entire GEMS backup CD-ROM(S) for both elections is the only way ... to undertake a complete audit."

In response to the request, DeKalb County advised Raffauf by letter that it would produce the requested CD-ROM on November 9, 2006. The county also noted, however, that it was going to utilize the letter to "notify the Secretary of State [and] the Attorney General ... of [its] impending release of the requested CD-ROM in the event they choose to take action." Further, the county refused to produce "documents or records that are not subject to production under the [*Open Records] Act*" and expressly reserved "any and all statutory exemptions from disclosure provided by *OCGA § 50-18-72*, and any and all other exemptions or protections provided by law, including **[***5]** but not limited to privileged and confidential documents."

On November 9, 2006, the Secretary of State objected to the open records request **[**471]** and filed a petition for a temporary restraining order ("TRO") and a verified complaint for a permanent injunction prohibiting DeKalb County from releasing the CD-ROM. After the trial court granted two TROs, [5] Smith intervened. The court

---

expired. Karen Handel became Secretary of State on January 8, 2007.

[2] "GEMS" is an acronym for a software program known as the "Global Election Management System," which is produced by Diebold Election Systems. "CD-ROM" is an acronym for "computer disk – read only memory."

[3] *OCGA § 21-2-500 (a)* states as follows:

> Immediately upon completing the returns required by this article, in the case of elections other than municipal elections, the superintendent shall deliver in sealed containers to the clerk of the superior court or, if designated by the clerk of the superior court, to the county records manager or other office or officer under the jurisdiction of a county governing authority which maintains or is responsible for records, as provided in *Code Section 50-18-99*, the **[***3]** used and void ballots and the stubs of all ballots used; one copy of the oaths of poll officers; and one copy of each numbered list of voters, tally paper, voting machine paper proof sheet, and return sheet involved in the primary or election. In addition, the superintendent shall deliver copies of the voting machine ballot labels, computer chips containing ballot tabulation programs, copies of computer records of ballot design, and similar items or an electronic record of the program by which votes are to be recorded or tabulated, which is captured prior to the election, and which is stored on some alternative medium such as a CD-ROM or floppy disk simultaneously with the programming of the PROM or other memory storage device. The clerk, county records manager, or the office or officer designated by the clerk shall hold such ballots and other documents under seal, unless otherwise directed by the superior court, for at least 24 months, after which time they shall be presented to the grand jury for inspection at its next meeting. Such ballots and other documents shall be preserved in the office of the clerk, county records manager, or officer designated by the clerk until the adjournment **[***4]** of such grand jury, and then they may be destroyed, unless otherwise provided by order of the superior court.

[4] *Ga. Comp. R. & Regs. r. 183-1-12-.02 (6)* states, in pertinent part, as follows:

> Storage of Returns. (a) After tabulating and consolidating the results, the election superintendent shall prepare a CD-ROM which shall contain a copy of the information contained on each memory card (PCMCIA card) which shall include all ballot images as well as vote totals and a copy of the consolidated returns from the election management system.

[5] The record shows that the court initially granted a TRO restraining DeKalb County from releasing the CD-ROM on November 9, 2006. The court granted a second TRO on

conducted a hearing on the petition for a permanent injunction, and the Secretary of State and Smith presented evidence and argument. The court **[*576]** permanently restrained and enjoined DeKalb County and Latimore from "releasing, disclosing, or providing to any person not authorized by law to obtain them copies of the pre-election and post-election CD-ROMs." Smith appeals from this order.

1. Smith claims that the trial court erred in finding that the Secretary of State had standing to object to his *Open Records Act* request. As the court found, however, the Secretary of State "is statutorily charged with the supervision of all elections in **[***6]** this State, and as such has a complete right to seek the Court's intervention in this matter." See *OCGA §§ 21-2-30* (creating the State Election Board and naming the Secretary of State as the board chair); *21-2-31* (duties of the State Election Board); *21-2-32* (authorizing the State Election Board to institute or intervene in court actions involving elections); *21-2-50 et seq.* (powers and duties of the Secretary of State regarding elections); *45-13-20 et seq.* (general duties of the Secretary of State); see also *Ga. Dept. of Natural Resources v. Theragenics Corp., 273 Ga. 724, 725 (545 SE2d 904) (2001)* (a corporation had the right to enjoin a state agency from allowing a third-party competitor to review the agency's file on the corporation, which included some of the corporation's trade secrets, after the third party filed a request with the agency under the *Open Records Act*).

2. Smith contends that the court erred in granting the permanent injunction. Smith claims that he is entitled to inspect the CD-ROM by running a copy on an independent computer which would enable him to examine the CD-ROM's computer codes to determine when various voting records were created and by whom, "to verify **[***7]** file formats, software versions, [and] file sizes" on the CD-ROM, and to look for evidence of irregularities resulting from election fraud and malfunctions of the electronic voting equipment and election software. [6]

> In determining whether the trial court's grant of a permanent injunction was proper, the standard of review on appeal is whether or not the trial court manifestly abused its discretion. A trial judge manifestly abuses his discretion when he grants an injunction adverse to a party without any evidence to support such judgment and contrary to the law and equity. Entry of a permanent injunction is appropriate in clear and urgent cases where there is a vital necessity to prevent a party from being damaged and left without an adequate remedy at law.

[*577] (Citations and punctuation omitted.) *City of Atlanta v. Southern States Police Benevolent Assn. &c., 276 Ga. App. 446, 458 (4) (623 SE2d 557) (2005)*. (1) We conclude that the court's ruling that Smith is not entitled to a copy of the CD-ROM under the *Open Records Act* is proper for several reasons.

Under Georgia's *Open Records Act*,

> [a]ll public records of an agency as defined in *subsection (a) of this Code* section, except those which by order of a court of this state or by law are prohibited or specifically exempted from being open to inspection by the general public, shall be open for a personal inspection by any citizen of this state at a reasonable time and place; and those in charge of such records shall not refuse this privilege to any citizen.

OCGA § 50-18-70 (b). As the trial court found, the Georgia Code provides that the designated custodian of a CD-ROM created by the county or municipal superintendent of an election must maintain it *under seal* following the election for at least 24 months, unless otherwise directed by the superior **[**472]** court. *OCGA § 21-2-500 (a)*; [7] see *Ga. Comp. R. & Regs. r. 183-1-12-.02 (6)* (storage of returns). The superior court in this case has not ordered that the seal be lifted as to the CD-ROM Smith seeks. Thus, because the CD-ROM is statutorily designated to be kept under seal, it is by law prohibited or specifically exempted from being open to inspection by the general public and, therefore, **[***9]** is not an open record subject to disclosure. *OCGA § 50-18-70 (b)*. As a result, the trial court did not abuse its discretion in granting the Secretary of State's petition for a permanent injunction prohibiting the custodian from

---

December 11, 2006.

[6] Although Smith does not have the GEMS software necessary to access the encrypted information on the CD-ROM, his witness claimed he could break **[***8]** the encryption codes with software from other sources.

[7] After a minimum of 24 months after an election, the custodian shall present the sealed voting records to the grand jury for inspection at its next meeting. *OCGA § 21-2-500 (a)*. After the grand jury adjourns, the custodian may retain the records under seal or destroy them, "unless otherwise provided by order of the superior court." Id.

opening the record in response to Smith's *Open Records Act* request.

In addition, the trial court found, based on evidence tendered by the Secretary of State, that release of the CD-ROM, which contains passwords, encryption codes, and other security information, would compromise election security. As a result, the trial court ruled that the CD-ROM was exempted from the *Open Records Act* on the alternative basis of the exemption for "material which if made public could compromise security against sabotage, criminal, or terroristic acts." *OCGA § 50-18-72 (a) (15) (A) (iv)*. See footnote 6, supra (regarding Smith's witness' claim that **[***10]** he could break the encryption codes with software from other sources). Although Smith argues that the **[*578]** State could copy the CD-ROM without including the passwords, encryption codes, and other security information, the *Open Records Act* specifically provides that the government agency is not required to create reports, summaries, or compilations that were not in existence at the time of the request. *OCGA § 50-18-70 (d)*. [8] Accordingly, the trial court did not abuse its discretion in granting the Secretary of State's petition for an injunction on this alternative basis.

In sum, the record supports the court's finding that Smith is not entitled to a copy of the CD-ROM under the *Open Records Act*.

3. Smith argues that the court improperly granted the TROs and that a prior judge to whom the case had been assigned improperly denied his motion to recuse. The record shows, however, that Smith **[***11]** was not a party to this action when the court granted the TROs or when it denied the motion to recuse. Further, the judge who denied his motion to recuse was no longer assigned to the case at the time of the hearing on the request for a permanent injunction or the court's ruling thereon. Thus, these allegations of error lack merit.

Judgment affirmed. Andrews, P. J., and Adams, J., concur.

---

[8] Notably, the evidence showed that DeKalb County has provided the voting records from the 2006 4th Congressional District primary to Smith, allowing his attorney to use a county computer that runs the necessary software so that he could review the records and providing him with print-outs of the information.

Joseph Kirk

From: Harvey, Chris <wharvey@sos.ga.gov>
Sent: Thursday, July 26, 2018 12:47 PM
To: 22ballance@gmail.com; acrosby@fayettecountyga.gov; adavis@co.newton.ga.us; adrienne-ray@peachcounty.net; adumas@monroecountygeorgia.com; aharper@troupco.org; AL.MCCRANIE@YAHOO.COM; ALASHIA.BROWN@YAHOO.COM; amantle@co.newton.ga.us; ann.russell@gmail.com; APHAGAN@CO.BANKS.GA.US; applingregdon@yahoo.com; Ashley.Peck@LumpkinCounty.GOV; ASMITH@BUTTSCOUNTY.ORG; Atcoelections@hotmail.com; b.peacock@crawfordcountyga.org; baldwinprobate@yahoo.com; bcochran@stephenscountyga.com; BDAWSON@UPSONCOUNTYGA.ORG; BELECTIONS@WINDSTREAM.NET; berlaseter@gmail.com; bgillis@warecounty.com; bhodges@charltoncountyga.gov; BLECKLEYVR@BLECKLEY.ORG; BLLuth@forsythco.com; bmwhite@co.camden.ga.us; BNABLE@HOUSTONCOUNTYGA.ORG; BOER.Supervisor@HancockCountyGA.gov; brookscoelections@windstream.net; burkereg@burkecounty-ga.gov; CACHENBACH.TOOMBS.ELECTIONS@GMAIL.COM; candlerprobate@gmail.com; carolyn03@windstream.net; CC.REGISTRAR@WINDSTREAM.NET; ccstephenstcpj@yahoo.com; Charlotte.Sosebee@athensclarkecounty.com; chattoogaelections@hotmail.com; chattoogaregistrar@gmail.com; cheard@decaturcountyga.gov; cindyreynolds@bryan-county.org; ckathleen@greenecountyga.gov; clairemoseley@gmail.com; Clayprobate@hotmail.com; CLHAGANS@WASHINGTONCOUNTYGA.GOV; clinchelections@windstream.net; cookelections@windstream.net; Cora.Wright@athensclarkecounty.com; cwinkler@murraycountyga.gov; cynthia.welch@rockdalecounty.org; DARIN.MCCOY@EVANSCOUNTY.ORG; DC.REGISTRAR.GA@HOTMAIL.COM; ddallas@classicsouth.net; Deb Cox; dholden@paulding.gov; DKILLINGSWORTH@JOHNSONCO.ORG; DOOLY.COUNTY.ELECTIONS@GMAIL.COM; DOROTHYHGLISSON@YAHOO.COM; DSTEPHENS@TWIGGSCOUNTY.US; Dwight.Brower@fultoncountyga.gov; ECHOLSCO.REGISTRAR@GMAIL.COM; ecprobate@hotmail.com; egale@darientel.net; ehamilton@dekalbcountyga.gov; elections@walkerga.us; ella.golden@libertycountyga.com; EVANSCOUNTYREGISTRAR@HOTMAIL.COM; fdavis@oconee.ga.us; fjones@fayettecountyga.gov; FRANKIE@GAWEBSERVICES.COM; gbaker@whitecounty.net; gchappelear@franklincountyga.com; GFERGUSON@DAWSONCOUNTY.ORG; GILMERPROBATE@ELLIJAY.COM; GNICKERSON@DOUGHERTY.GA.US; greenw@floydcountyga.org; grigby@carrollcountyga.com; HARPERH@DLCGA.COM; HCELECTIONS@BELLSOUTH.NET; HWMS46@YAHOO.COM; Janine.Eveler@cobbcounty.org; jasperprobate@bellsouth.net; jdoran@morganga.org; jduff@carrollcountyga.com; JDYCRTR@YAHOO.COM; jeffdaviselections@gmail.com; jelogan@jacksoncountygov.com; JENKINSCOUNTYREG@BELLSOUTH.NET; JJONES@COMSOUTH.NET; jovall2@yahoo.com; jregistrar@bellsouth.net; jroberts@pickenscountyga.gov; JSCOGGINS@COWETA.GA.US; jstone@oconee.ga.us; JUDGEMCG@YAHOO.COM; judgenation@oglethorpecountyga.gov; judgerodgers@planttel.net; jwatson@maconbibb.us; karnold@waynecountyga.us; KCURRY@EMANUELCO-GA.GOV; KHarris@CANDLERCO-GA.GOV; kharvey@dougherty.ga.us; kirkj@bartowga.org; klewis@benhillcounty.com; KPOWELL@BLECKLEY.ORG; Kristi.Royston@gwinnettcounty.com; kstancil@cherokeega.com; kwarren@monroecountygeorgia.com; lamarcountyregistrars@yahoo.com; laniercountyvotes@yahoo.com; LANIERPROBATE1@WINDSTREAM.NET; LBailey@augustaga.gov; lbolton@lincolncountyga.com;

To: leah.williamson@piercecountyga.gov; lellison@habershamga.com; LFULTON@CO.DOUGLAS.GA.US; LISA@UGOCCC.COM; lmanning@whitecounty.net; longcountyelections@gmail.com; lsampson@murraycountyga.gov; lwalton@decaturcountyga.gov; Lwilliams@warecounty.com; Lynn Ledford; MACOBOER@WINDSTREAM.NET; maconner@fannincountyga.org; maddox.denise2@gmail.com; malinda.butler@gradycountyga.gov; marion_hatton@hotmail.com; MARIONCOUNTYELECT@GMAIL.COM; MBSmith@forsythco.com; mcouch@glynncounty-ga.gov; mfranklin@barrowga.org; mhammontree@whitfieldcountyga.com; MHOWARD.TALBOT@GMAIL.COM; millerprobate@gmail.com; mistyhayes@coffeecountygov.com; mjclemons1961@yahoo.com; mkidd@co.douglas.ga.us; mridley@spaldingcounty.com; MWAY@WINDSTREAM.NET; NBOREN@COLUMBUSGA.ORG; ngay@columbiacountyga.gov; OMORGAN@EFFINGHAMCOUNTY.ORG; p.threadgill@meriwethercountyga.gov; paulamc@ccboc.com; pepparhcelections@gmail.com; PERKINSB@CRISPCOUNTY.COM; phyllis.wheeler3@thomson-mcduffie.net; pikeproburg@yahoo.com; PLANIERJONES@BULLOCHCOUNTY.NET; pnix@hallcounty.org; PRELEFORD@UPSONCOUNTYGA.ORG; PROBATE8@GMAIL.COM; PROBATEELECT@PLANTERS.NET; projudgeholder@windstream.net; QUITCO8@EUFAULA.RR.COM; quitcojudge@eufaula.rr.com; Ralph.Jones@fultoncountyga.gov; RBRADY@SUMTERCOUNTYGA.US; rbridges@chathamcounty.org; rcsweatt@co.camden.ga.us; registrar@ellijay.com; REGISTRARS@DLCGA.COM; REGISTRARS@MILLERCOUNTYGA.COM; REGISTRARS_SCHLEY@YAHOO.COM; registrars131@yahoo.com; renee.phifer@rockdalecountyga.gov; Richard.Barron@fultoncountyga.gov; rkiefer@greenecountyga.gov; RMOXSAND@HOTMAIL.COM; rwebb@hartcountyga.gov; sandraveal13@gmail.com; schamblin@pikecoga.com; SDoorenbos@morganga.org; seminoleprobate@gmail.com; SGRAY@JEFFERSONCOUNTYGA.GOV; shauna.dozier@claytoncountyga.gov; SHICKS@GORDONCOUNTY.ORG; SJARRETT@HARRISCOUNTYGA.GOV; ssgerman@chathamcounty.org; susancarol1952@gmail.com; TACLAY@windstream.net; tadams@heardcountyga.com; tammy.whitmire@rabuncounty.ga.gov; TATTNALL_ELECTIONS_24@YAHOO.COM; TBLACK@STEWARTCOUNTYGA.GOV; tcmail@rose.net; TELFAIR.REGISTRAR@HOTMAIL.COM; TELFAIRPROBATE@WINDSTREAM.NET; TGCOUNTY@GMAIL.COM; thomascharping@wilkescountyga.org; TJ4TREUTLEN@YAHOO.COM; tlunsford@co.henry.ga.us; tonya.moore@catoosa.com; townssupervisor@yahoo.com; Tracy Dean; Travis Doss; tsargent@hallcounty.org; TSTRANGE@WILKINSONCOUNTY.NET; Tthornton@waynecountyga.us; tuckerlaurabeth@gmail.com; tvaughan@dadecounty-ga.gov; UCREGISTRAR@UNIONGOV.COM; uge3125@uga.edu; vjohnson@lee.ga.us; votecw@elberton.net; voterreg@btconline.net; VOTERREGISTRAR@BULLOCHCOUNTY.NET; voterregistration@windstream.net; VOTETAYLOR@YAHOO.COM; VRMONTGOMERY@YAHOO.COM; warrenvotereg@classicsouth.net; wcboe.supervisor@gmail.com; wcprobate@classicsouth.net; WCREGISTRARS@WINDSTREAM.NET; WEBSTERFINANCE@WINDSTREAM.NET; weslewis@ccboc.com; WILCOX2115@WINDSTREAM.NET; wilkescovoter@hotmail.com; worthelechair@hotmail.com; WPROBATE@HOTMAIL.COM

Cc: Harvey, Chris

Subject: Import OEB Posted in Firefly

All,

We have posted an important OEB in Firefly concerning information about cybersecurity and an update on the activity of foreign operatives on elections webpages in Georgia in 2016, as mentioned in the Mueller indictment earlier this month.

Please read the OEB and assert the imperative to take cyber security very seriously.
Email integrity and spear-phishing are areas that need constant attention.

We will be providing more resources in the future.

You are welcome to call me if you have questions about any of these matters.

Chris Harvey
Elections Director, Georgia Secretary of State

404-657-5380 DIRECT
404-985-6351 MOBILE

OFFICIAL ELECTION BULLETIN

July 26, 2018

TO: **County Election Officials and County Registrars**

FROM: **Chris Harvey, Elections Division Director**

RE: **Suspected Russian Operative Activity**

On July 13, Special Counsel Robert Mueller released an indictment that alleges that, on or about October 28, 2016, a suspected Russian operative "visited the websites of certain counties in Georgia, Iowa, and Florida to identify vulnerabilities."

Since the indictment was released, we have been working closely with the Department of Homeland Security to obtain more information. Now that we have more details, we are sharing with you what we have learned.

In 2016, the suspected Russian operative visited two Georgia county webpages. Those counties have been separately notified. There is no evidence that either of the county webpages were compromised as a result of this activity. Both webpages showed general, public information about elections. The federal government does not have information as to what actions the operative took in order "to identify vulnerabilities," but they assume that the operative was conducting research designed to assist future potential operations—for example, looking for email addresses to conduct spear phishing campaigns or attempting to understand what specific technology or processes are used in our election system. The Secretary of State's Office agrees with this assumption.

Georgia's election systems remain secure, and we continue to prioritize our security in this environment. However, I want to remind each of you that, as election officials, you are all high-value targets. Be vigilant. Have a security mindset. Many of you have received physical security assessments from DHS, and the report is that these have been helpful. DHS also offers on-site network security assessments. On-site security assessments can be requested through ncciccusomterservice@hq.dhs.gov. The wait time for the network security assessments through DHS can be lengthy. Private sector vendors are also available without a lengthy wait. If your county wants to do a physical security or network security assessment, I will discuss the process with you and offer any support that our office can provide.

OFFICIAL ELECTION BULLETIN

August 1, 2018

TO: **County Election Officials and County Registrars**

FROM: **Chris Harvey, Elections Division Director**

RE: **Response to Coalition for Good Governance Communication**

Dear County Commissioners and Officials,

I am writing to you as the State of Georgia's Elections Director, a position I have held since July 2015. From August 2007 until July 2015, I was the Chief Investigator and Deputy Inspector General for the Secretary of State's office, investigating, among other items, potential violations of state election law. For over a decade, it has been my job to be intimately familiar with both Georgia election law, systems, processes, and procedures.

Before joining the Secretary of State's office, I was the Director of the Cold Case Homicide Unit with the Fulton County District Attorney's office where I investigated previously unsolved homicides. Prior to that role, I was the Chief Investigator with the DeKalb County District Attorney's Office where I led investigations in all crimes, including public corruption. Over my career in law enforcement, it has been my intention to serve Georgia by promoting public safety, security and fidelity to the law.

Throughout my tenure at the Secretary of State's office, election security has been a top priority for me personally, as it is for the entire Secretary of State's office and county election officials. Now more than ever, and especially since the election of 2016, voting security is featuring more prominently as a topic of national conversation. However, it has been a way of life in the Secretary of State's office for far longer. I write to you today to explain some of the protections that we, along with county election officials, have in place to ensure that Georgia's elections are secure and ask for your assistance in continuing to ensure secure elections in our state.

Elections in Georgia are a partnership between the state and the counties. County election officials run elections while the Secretary of State's office maintains the voter registration database and provides support to the counties. We work with your county election officials every day, and these hard-working public servants are truly the linchpin of our democracy.

Long before the public spotlight turned to the realm of elections, we recognized the real threat of people and entities - both foreign and domestic – seeking to interfere with our electoral process.

To combat this threat, we work with federal, state, local, and private sector partners every day, and we are continually adding additional levels of both cyber and physical security to Georgia's election system. It is our duty to provide Georgians with the opportunity to vote on a secure and reliable voting system, which we regularly test to ensure ongoing compliance with state law and State Election Board rules.

Georgia's election system consists of many components, including the voter registration system, election management system, voting machines, and election night reporting website. Strict security mechanisms surround each component. These safeguards include, but are not limited to, frequent password changes, brute force and inactivity account disabling, and two-factor authentication. Many people are pleasantly surprised to hear that Georgia builds its encrypted ballot databases on machines which are never connected to the internet—a safeguard which many other states have not yet implemented. We also deploy cybersecurity protections, secure armed transport of election materials, and physical security for our voting machines. Your county election officials are familiar with these processes and treat them with the utmost importance.

Recently, some county boards have received communications from parties who filed a federal lawsuit against Georgia to stop the use of voting machines – Direct Recording Electronic (DRE) equipment – and demand hand-counted paper ballots. In these communications to you, they mistakenly cite a state law which was superseded by a newer law for the assertion that counties can unilaterally elect to stop using DRE voting equipment. Their assertion is not an accurate statement of Georgia law.

In 2003, Georgia moved to a state-wide, unified system in 2003. O.C.G.A. § 21-2-300 (a) states, "Provided that the General Assembly specifically appropriates funding to the Secretary of State to implement this subsection, the equipment used for casting and counting votes in county, state, and federal elections shall, by the July, 2004, primary election and afterwards, be the same in each county in this state and shall be provided to each county by the state, as determined by the Secretary of State." Further, O.C.G.A. § 21-2-381 requires absentee in-person ballots (early voting) to be on a DRE and O.C.G.A. § 21-2-379.7, which requires at least one DRE unit accessible to handicapped voters to be placed in each precinct, and State Election Board rules align with both of these statutes.

There are some who believe that because the current DRE machines are fully electronic, there is no way to verify that voter selections match the vote count's output. This belief is not true. There are numerous ways to ensure that our voting machines are accurately counting votes, and election officials test and demonstrate the accuracy of these machines through logic and accuracy testing before every single use. Last year, the state also conducted a re-examination of the voting machines to ensure accuracy. In each of the three selected counties, each machine's output exactly matched its input on simulated election day conditions. Furthermore, on election days in 2018, the Secretary of State's office conducts parallel testing, which means we take an actual county's ballot database and run a mock election to ensure that output matches the ballot selections. In each instance, the machine's output has exactly matched the selections. We have never taken accuracy for granted. It is constantly tested and re-tested.

There is a provision of Georgia law that allows the state to move to paper ballots in the event that the machines are "inoperable or unsafe." If we ever reach a point where our office feels that these

machines cannot be trusted to accurately deliver election results, we will invoke this statutory provision. To this day, there is no credible evidence that our election process is anything except secure and accurate.

While we are confident in the integrity of our elections, we remain vigilant and committed to ensuring that the confidence of Georgia voters in their elections and government is well-deserved. The Secretary of State's commitment to constant vigilance is why we have supported a move towards a new voting system to replace the current, aging system in a responsible fashion. This year, Secretary Kemp appointed the bi-partisan Secure, Accessible, and Fair Elections (SAFE) Commission, which consists of numerous county election officials, legislators, election law experts, a cybersecurity expert, and an accessibility expert. The SAFE Commission, working with our office, will present recommendations to the General Assembly by this January on how to responsibly move to a new system.

As county officials, we recognize the role that you play in keeping our system secure and accurate. The Secretary of State's Office values our county partners who work hand-in-hand with county elections boards and officials to run Georgia's elections. Thank you for your continued support and dedication to secure elections in Georgia. Please feel free to contact me directly with any questions.

Sincerely,

Chris Harvey

State Elections Director

OFFICIAL ELECTION BULLETIN

August 9, 2018

TO: **County Election Officials and County Registrars**

FROM: **Chris Harvey, Elections Division Director**

RE: **Physical Security Assessments Offered by Dept. of Homeland Security**

This is a reminder and an encouragement for election officials to consider contacting the U.S. Department of Homeland Security (DHS) to conduct a Physical Security Assessment (PSA) on your election offices, storage facilities, or other locations in your county where election equipment or infrastructure is used or stored.

The PSAs are conducted at no cost to your county or office and can be completed in a few hours. You will be provided with suggestions for improvements to your already existing security systems and protocols.

Many counties of various sizes and resources have already taken advantage of this program, and I have heard very positive feedback about the process and interaction with DHS on these PSAs.

Dennis Mott, from DHS, is looking forward to hearing from all counties that are interested in completing a PSA in the lead-up to the 2018 General Election.

Please contact Dennis Mott directly by phone at **202-407-2793** or by email at dennis.mott@hq.dhs.gov

If you have questions about these PSAs or other security issues, please contact me directly.

OFFICIAL ELECTION BULLETIN

August 17, 2018

TO: **County Election Officials and County Registrars**

FROM: **Chris Harvey, Elections Division Director**

RE: **Phishing Attempt**

On 08-17-18, at approximately 11:12 AM, the Secretary of State's anti-phishing defenses identified an email that appeared to come from Nancy Boren, Muscogee County Election Director. The email offered an opportunity to shop at Walmart and a link for the recipient to click. Our office immediately contacted Nancy Boren directly and confirmed that she had not sent the email. She had already been alerted to the suspicious email and was working with her IT office to investigate the situation.

Our office activated our incidence response plans and immediately coordinated investigative and protective efforts with all of our security partners, including those in the federal government. Our office contacted Dept. of Homeland Security and MS-ISAC to advise them of the situation, and we took additional measures to make sure that ENET was secure. In addition, we sent out Buzz Posts and emails to county election officials to be on the alert for that or any other suspicious emails.

Muscogee County IT is working with the Department of Homeland Security and MS-ISAC to determine the nature and source of the apparent phishing attempt. Early indicators are that this was not specifically targeting the Muscogee County Elections Office.

This is a timely reminder that email phishing attempts remain one of the more popular and effective methods of cyber attack. It is imperative that all county offices train their employees on the nature of email phishing attempts and to exercise great care when interacting with email, especially email with embedded links or attachments. The additional security features added to ENET, such as two-factor authentication, continue to provide protection for ENET and other cyber systems, but the individual user still must use consistent caution when interacting with others through email and other cyber communications.

If you have questions about this situation, please contact the Secretary of State's Office.

Joseph Kirk

From: Harvey, Chris <wharvey@sos.ga.gov>
Sent: Tuesday, September 18, 2018 11:59 AM
To: 22ballance@gmail.com; acrosby@fayettecountyga.gov; adavis@co.newton.ga.us; adrienne-ray@peachcounty.net; adumas@monroecountygeorgia.com; aharper@troupco.org; AL.MCCRANIE@YAHOO.COM; ALASHIA.BROWN@YAHOO.COM; amantle@co.newton.ga.us; ann.russell@gmail.com; APHAGAN@CO.BANKS.GA.US; applingregdon@yahoo.com; Ashley.Peck@LumpkinCounty.GOV; ASMITH@BUTTSCOUNTY.ORG; Atcoelections@hotmail.com; b.peacock@crawfordcountyga.org; baldwinprobate@yahoo.com; bcochran@stephenscountyga.com; BDAWSON@UPSONCOUNTYGA.ORG; BELECTIONS@WINDSTREAM.NET; berlaseter@gmail.com; bgillis@warecounty.com; bhodges@charltoncountyga.gov; BLECKLEYVR@BLECKLEY.ORG; BLLuth@forsythco.com; bmwhite@co.camden.ga.us; BNABLE@HOUSTONCOUNTYGA.ORG; BOER.Supervisor@HancockCountyGA.gov; brookscoelections@windstream.net; burkereg@burkecounty-ga.gov; CACHENBACH.TOOMBS.ELECTIONS@GMAIL.COM; candlerprobate@gmail.com; carolyn03@windstream.net; CC.REGISTRAR@WINDSTREAM.NET; ccstephenstcpj@yahoo.com; Charlotte.Sosebee@athensclarkecounty.com; chattoogaelections@hotmail.com; chattoogaregistrar@gmail.com; cheard@decaturcountyga.gov; cindyreynolds@bryan-county.org; ckathleen@greenecountyga.gov; clairemoseley@gmail.com; Clayprobate@hotmail.com; CLHAGANS@WASHINGTONCOUNTYGA.GOV; clinchelections@windstream.net; cookelections@windstream.net; Cora.Wright@athensclarkecounty.com; cwinkler@murraycountyga.gov; cynthia.welch@rockdalecounty.org; DARIN.MCCOY@EVANSCOUNTY.ORG; DC.REGISTRAR.GA@HOTMAIL.COM; ddallas@classicsouth.net; Deb Cox; dholden@paulding.gov; DKILLINGSWORTH@JOHNSONCO.ORG; DOOLY.COUNTY.ELECTIONS@GMAIL.COM; DOROTHYHGLISSON@YAHOO.COM; DSTEPHENS@TWIGGSCOUNTY.US; Dwight.Brower@fultoncountyga.gov; ECHOLSCO.REGISTRAR@GMAIL.COM; ecprobate@hotmail.com; egale@darientel.net; ehamilton@dekalbcountyga.gov; elections@walkerga.us; ella.golden@libertycountyga.com; EVANSCOUNTYREGISTRAR@HOTMAIL.COM; fdavis@oconee.ga.us; fjones@fayettecountyga.gov; FRANKIE@GAWEBSERVICES.COM; gbaker@whitecounty.net; gchappelear@franklincountyga.com; GFERGUSON@DAWSONCOUNTY.ORG; GILMERPROBATE@ELLIJAY.COM; GNICKERSON@DOUGHERTY.GA.US; greenw@floydcountyga.org; grigby@carrollcountyga.com; HARPERH@DLCGA.COM; HCELECTIONS@BELLSOUTH.NET; HWMS46@YAHOO.COM; Janine.Eveler@cobbcounty.org; jasperprobate@bellsouth.net; jdoran@morganga.org; jduff@carrollcountyga.com; JDYCRTR@YAHOO.COM; jeffdaviselections@gmail.com; jelogan@jacksoncountygov.com; JENKINSCOUNTYREG@BELLSOUTH.NET; JJONES@COMSOUTH.NET; jovall2@yahoo.com; jregistrar@bellsouth.net; jroberts@pickenscountyga.gov; JSCOGGINS@COWETA.GA.US; jstone@oconee.ga.us; JUDGEMCG@YAHOO.COM; judgenation@oglethorpecountyga.gov; judgerodgers@planttel.net; jwatson@maconbibb.us; karnold@waynecountyga.us; KCURRY@EMANUELCO-GA.GOV; KHarris@CANDLERCO-GA.GOV; kharvey@dougherty.ga.us; kirkj@bartowga.org; klewis@benhillcounty.com; KPOWELL@BLECKLEY.ORG; Kristi.Royston@gwinnettcounty.com; kstancil@cherokeega.com; kwarren@monroecountygeorgia.com; lamarcountyregistrars@yahoo.com; laniercountyvotes@yahoo.com; LANIERPROBATE1@WINDSTREAM.NET; LBailey@augustaga.gov; lbolton@lincolncountyga.com;

To: leah.williamson@piercecountyga.gov; lellison@habershamga.com; LFULTON@CO.DOUGLAS.GA.US; LISA@UGOCCC.COM; lmanning@whitecounty.net; longcountyelections@gmail.com; lsampson@murraycountyga.gov; lwalton@decaturcountyga.gov; Lwilliams@warecounty.com; Lynn Ledford; MACOBOER@WINDSTREAM.NET; maconner@fannincountyga.org; maddox.denise2@gmail.com; malinda.butler@gradycountyga.gov; marion_hatton@hotmail.com; MARIONCOUNTYELECT@GMAIL.COM; MBSmith@forsythco.com; mcouch@glynncounty-ga.gov; mfranklin@barrowga.org; mhammontree@whitfieldcountyga.com; MHOWARD.TALBOT@GMAIL.COM; millerprobate@gmail.com; mistyhayes@coffeecountygov.com; mjclemons1961@yahoo.com; mkidd@co.douglas.ga.us; mridley@spaldingcounty.com; MWAY@WINDSTREAM.NET; NBOREN@COLUMBUSGA.ORG; ngay@columbiacountyga.gov; OMORGAN@EFFINGHAMCOUNTY.ORG; p.threadgill@meriwethercountyga.gov; paulamc@ccboc.com; pepparhcelections@gmail.com; PERKINSB@CRISPCOUNTY.COM; phyllis.wheeler3@thomson-mcduffie.net; pikeproburg@yahoo.com; PLANIERJONES@BULLOCHCOUNTY.NET; pnix@hallcounty.org; PRELEFORD@UPSONCOUNTYGA.ORG; PROBATE8@GMAIL.COM; PROBATEELECT@PLANTERS.NET; projudgeholder@windstream.net; QUITCO8@EUFAULA.RR.COM; quitcojudge@eufaula.rr.com; Ralph.Jones@fultoncountyga.gov; RBRADY@SUMTERCOUNTYGA.US; rbridges@chathamcounty.org; rcsweatt@co.camden.ga.us; registrar@ellijay.com; REGISTRARS@DLCGA.COM; REGISTRARS@MILLERCOUNTYGA.COM; REGISTRARS_SCHLEY@YAHOO.COM; registrars131@yahoo.com; renee.phifer@rockdalecountyga.gov; Richard.Barron@fultoncountyga.gov; rkiefer@greenecountyga.gov; RMOXSAND@HOTMAIL.COM; rwebb@hartcountyga.gov; sandraveal13@gmail.com; schamblin@pikecoga.com; SDoorenbos@morganga.org; seminoleprobate@gmail.com; SGRAY@JEFFERSONCOUNTYGA.GOV; shauna.dozier@claytoncountyga.gov; SHICKS@GORDONCOUNTY.ORG; SJARRETT@HARRISCOUNTYGA.GOV; ssgerman@chathamcounty.org; susancarol1952@gmail.com; TACLAY@windstream.net; tadams@heardcountyga.com; tammy.whitmire@rabuncounty.ga.gov; TATTNALL_ELECTIONS_24@YAHOO.COM; TBLACK@STEWARTCOUNTYGA.GOV; tcmail@rose.net; TELFAIR.REGISTRAR@HOTMAIL.COM; TELFAIRPROBATE@WINDSTREAM.NET; TGCOUNTY@GMAIL.COM; thomascharping@wilkescountyga.org; TJ4TREUTLEN@YAHOO.COM; tlunsford@co.henry.ga.us; tonya.moore@catoosa.com; townssupervisor@yahoo.com; Tracy Dean; Travis Doss; tsargent@hallcounty.org; TSTRANGE@WILKINSONCOUNTY.NET; Tthornton@waynecountyga.us; tuckerlaurabeth@gmail.com; tvaughan@dadecounty-ga.gov; UCREGISTRAR@UNIONGOV.COM; uge3125@uga.edu; vjohnson@lee.ga.us; votecw@elberton.net; voterreg@btconline.net; VOTERREGISTRAR@BULLOCHCOUNTY.NET; voterregistration@windstream.net; VOTETAYLOR@YAHOO.COM; VRMONTGOMERY@YAHOO.COM; warrenvotereg@classicsouth.net; wcboe.supervisor@gmail.com; wcprobate@classicsouth.net; WCREGISTRARS@WINDSTREAM.NET; WEBSTERFINANCE@WINDSTREAM.NET; weslewis@ccboc.com; WILCOX2115@WINDSTREAM.NET; wilkescovoter@hotmail.com; worthelechair@hotmail.com; WPROBATE@HOTMAIL.COM

Cc: Harvey, Chris

Subject: Communication Regarding U.S. District Judge's Order

On September 17, 2018, U.S. District Court Judge Amy Totenberg issued an order denying the plaintiffs' request that all

counties in Georgia be required to use paper ballots for the November 6, 2018 general election. This means that the November general election will go forward as planned using the regular procedures and equipment (DREs) that we have been using.

I want to share a few thoughts regarding these recent events.

1. The prioritization of election security has never been more important. Our office has been stressing the need for security at all levels. Cyber/internet security as well as physical security of buildings and voting equipment must remain a top priority for every single person who interacts with the voting system, whether that person is the county election director or a temporary poll worker. Everyone should be at a heightened level of awareness for anything unusual or suspicious.

2. There may be increases in requests for mailed absentee ballots from individuals who are concerned about voting on DREs. You should consider this factor when ordering absentee ballots and associated supplies, and monitor your supply in case you see the need to restock your supplies. This possible heightened demand will require your offices to be flexible and responsive in terms of being able to meet all requests for absentee ballots on a timely basis as required by SEB Rule:

   Rule 183-1-14-.11 Mailing and Issuance of Ballots
   During early voting, as additional applicants for absentee ballots are determined to be eligible, the board of registrars or absentee ballot clerk shall mail or issue official absentee ballots to such additional applicants immediately upon determining their eligibility. The board or clerk shall make such determination and mail or issue official absentee ballots to such additional eligible applicants within 3 business days after receiving the absentee ballot applications.

3. We have noted an increase in paper voter registration applications arriving in our office. We are distributing these applications to you regularly, and I am hearing that counties are seeing an increase in paper voter registration applications. I encourage you to continue to process these applications as efficiently as possible so that new voters can check their registration status online and be confident that they can vote in the general election.

Please continue to provide the best service that all voters in Georgia deserve and need, and let me know if our office can provide you with assistance.

Chris Harvey
Elections Director, Georgia Secretary of State

404-657-5380 DIRECT
404-985-6351 MOBILE

Joseph Kirk

From: DoNotReply@sos.ga.gov
Sent: Wednesday, September 19, 2018 5:25 PM
To: DoNotReply@sos.ga.gov
Subject: New Written Resources on Election Security Available on Firefly

A new discussion has
been posted in The Buzz by Harvey, Chris on 9/19/2018 5:16 PM

We have placed two new resources on Firefly under Official Communications>Election Security General that provide additional information about election security.

The first is a memo describing various ways individuals or other entities could attempt to interfere with elections.

The Second resource is a handbook that is a glossary of terms that one might encounter when reading about elections and security issues.

Keep in mind that these resources are written to election officials generally and may or may not contain information that is specifically relevant to Georgia and our laws, equipment, and practices. Remember that nothing in these communications supersedes Georgia law, SEB rules, or Secretary of State policies and practices. Election law and practices vary widely by state, so disregard information that is not relevant to Georgia.

If you have questions about any of these resources or information contained therein, please contact our office.

Chris Harvey

Secretary of State's Office

Joseph Kirk

From: Harvey, Chris <wharvey@sos.ga.gov>
Sent: Tuesday, October 2, 2018 3:48 PM
To: 22ballance@gmail.com; acrosby@fayettecountyga.gov; adavis@co.newton.ga.us; adrienne-ray@peachcounty.net; adumas@monroecountygeorgia.com; aharper@troupco.org; AL.MCCRANIE@YAHOO.COM; ALASHIA.BROWN@YAHOO.COM; amantle@co.newton.ga.us; ann.russell@gmail.com; APHAGAN@CO.BANKS.GA.US; applingregdon@yahoo.com; Ashley.Peck@LumpkinCounty.GOV; ASMITH@BUTTSCOUNTY.ORG; Atcoelections@hotmail.com; b.peacock@crawfordcountyga.org; baldwinprobate@yahoo.com; bcochran@stephenscountyga.com; BDAWSON@UPSONCOUNTYGA.ORG; BELECTIONS@WINDSTREAM.NET; berlaseter@gmail.com; bgillis@warecounty.com; bhodges@charltoncountyga.gov; BLECKLEYVR@BLECKLEY.ORG; BLLuth@forsythco.com; bmwhite@co.camden.ga.us; BNABLE@HOUSTONCOUNTYGA.ORG; BOER.Supervisor@HancockCountyGA.gov; brookscoelections@windstream.net; burkereg@burkecounty-ga.gov; CACHENBACH.TOOMBS.ELECTIONS@GMAIL.COM; candlerprobate@gmail.com; carolyn03@windstream.net; CC.REGISTRAR@WINDSTREAM.NET; ccstephenstcpj@yahoo.com; Charlotte.Sosebee@athensclarkecounty.com; chattoogaelections@hotmail.com; chattoogaregistrar@gmail.com; cheard@decaturcountyga.gov; cindyreynolds@bryan-county.org; ckathleen@greenecountyga.gov; clairemoseley@gmail.com; Clayprobate@hotmail.com; CLHAGANS@WASHINGTONCOUNTYGA.GOV; clinchelections@windstream.net; cookelections@windstream.net; Cora.Wright@athensclarkecounty.com; cwinkler@murraycountyga.gov; cynthia.welch@rockdalecounty.org; DARIN.MCCOY@EVANSCOUNTY.ORG; DC.REGISTRAR.GA@HOTMAIL.COM; ddallas@classicsouth.net; Deb Cox; dholden@paulding.gov; DKILLINGSWORTH@JOHNSONCO.ORG; DOOLY.COUNTY.ELECTIONS@GMAIL.COM; DOROTHYHGLISSON@YAHOO.COM; DSTEPHENS@TWIGGSCOUNTY.US; Dwight.Brower@fultoncountyga.gov; ECHOLSCO.REGISTRAR@GMAIL.COM; ecprobate@hotmail.com; egale@darientel.net; ehamilton@dekalbcountyga.gov; elections@walkerga.us; ella.golden@libertycountyga.com; EVANSCOUNTYREGISTRAR@HOTMAIL.COM; fdavis@oconee.ga.us; fjones@fayettecountyga.gov; FRANKIE@GAWEBSERVICES.COM; gbaker@whitecounty.net; gchappelear@franklincountyga.com; GFERGUSON@DAWSONCOUNTY.ORG; GILMERPROBATE@ELLIJAY.COM; GNICKERSON@DOUGHERTY.GA.US; greenw@floydcountyga.org; grigby@carrollcountyga.com; HARPERH@DLCGA.COM; HCELECTIONS@BELLSOUTH.NET; HWMS46@YAHOO.COM; Janine.Eveler@cobbcounty.org; jasperprobate@bellsouth.net; jdoran@morganga.org; jduff@carrollcountyga.com; JDYCRTR@YAHOO.COM; jeffdaviselections@gmail.com; jelogan@jacksoncountygov.com; JENKINSCOUNTYREG@BELLSOUTH.NET; JJONES@COMSOUTH.NET; jovall2@yahoo.com; jregistrar@bellsouth.net; jroberts@pickenscountyga.gov; JSCOGGINS@COWETA.GA.US; jstone@oconee.ga.us; JUDGEMCG@YAHOO.COM; judgenation@oglethorpecountyga.gov; judgerodgers@planttel.net; jwatson@maconbibb.us; karnold@waynecountyga.us; KCURRY@EMANUELCO-GA.GOV; KHarris@CANDLERCO-GA.GOV; kharvey@dougherty.ga.us; kirkj@bartowga.org; klewis@benhillcounty.com; KPOWELL@BLECKLEY.ORG; Kristi.Royston@gwinnettcounty.com; kstancil@cherokeega.com; kwarren@monroecountygeorgia.com; lamarcountyregistrars@yahoo.com; laniercountyvotes@yahoo.com; LANIERPROBATE1@WINDSTREAM.NET; LBailey@augustaga.gov; lbolton@lincolncountyga.com;

To: leah.williamson@piercecountyga.gov; lellison@habershamga.com; LFULTON@CO.DOUGLAS.GA.US; LISA@UGOCCC.COM; lmanning@whitecounty.net; longcountyelections@gmail.com; lsampson@murraycountyga.gov; lwalton@decaturcountyga.gov; Lwilliams@warecounty.com; Lynn Ledford; MACOBOER@WINDSTREAM.NET; maconner@fannincountyga.org; maddox.denise2@gmail.com; malinda.butler@gradycountyga.gov; marion_hatton@hotmail.com; MARIONCOUNTYELECT@GMAIL.COM; MBSmith@forsythco.com; mcouch@glynncounty-ga.gov; mfranklin@barrowga.org; mhammontree@whitfieldcountyga.com; MHOWARD.TALBOT@GMAIL.COM; millerprobate@gmail.com; mistyhayes@coffeecountygov.com; mjclemons1961@yahoo.com; mkidd@co.douglas.ga.us; mridley@spaldingcounty.com; MWAY@WINDSTREAM.NET; NBOREN@COLUMBUSGA.ORG; ngay@columbiacountyga.gov; OMORGAN@EFFINGHAMCOUNTY.ORG; p.threadgill@meriwethercountyga.gov; paulamc@ccboc.com; pepparhcelections@gmail.com; PERKINSB@CRISPCOUNTY.COM; phyllis.wheeler3@thomson-mcduffie.net; pikeproburg@yahoo.com; PLANIERJONES@BULLOCHCOUNTY.NET; pnix@hallcounty.org; PRELEFORD@UPSONCOUNTYGA.ORG; PROBATE8@GMAIL.COM; PROBATEELECT@PLANTERS.NET; projudgeholder@windstream.net; QUITCO8@EUFAULA.RR.COM; quitcojudge@eufaula.rr.com; Ralph.Jones@fultoncountyga.gov; RBRADY@SUMTERCOUNTYGA.US; rbridges@chathamcounty.org; rcsweatt@co.camden.ga.us; registrar@ellijay.com; REGISTRARS@DLCGA.COM; REGISTRARS@MILLERCOUNTYGA.COM; REGISTRARS_SCHLEY@YAHOO.COM; registrars131@yahoo.com; renee.phifer@rockdalecountyga.gov; Richard.Barron@fultoncountyga.gov; RMOXSAND@HOTMAIL.COM; rwebb@hartcountyga.gov; sandraveal13@gmail.com; schamblin@pikecoga.com; SDoorenbos@morganga.org; seminoleprobate@gmail.com; SGRAY@JEFFERSONCOUNTYGA.GOV; shauna.dozier@claytoncountyga.gov; SHICKS@GORDONCOUNTY.ORG; SJARRETT@HARRISCOUNTYGA.GOV; ssgerman@chathamcounty.org; susancarol1952@gmail.com; TACLAY@windstream.net; tadams@heardcountyga.com; tammy.whitmire@rabuncounty.ga.gov; TATTNALL_ELECTIONS_24@YAHOO.COM; tcmail@rose.net; TELFAIR.REGISTRAR@HOTMAIL.COM; TELFAIRPROBATE@WINDSTREAM.NET; TGCOUNTY@GMAIL.COM; thomascharping@wilkescountyga.org; TJ4TREUTLEN@YAHOO.COM; tlunsford@co.henry.ga.us; Todd Black (tblack.randolphcounty@gmail.com); tonya.moore@catoosa.com; townssupervisor@yahoo.com; Tracy Dean; Travis Doss; tsargent@hallcounty.org; TSTRANGE@WILKINSONCOUNTY.NET; Tthornton@waynecountyga.us; tuckerlaurabeth@gmail.com; tvaughan@dadecounty-ga.gov; UCREGISTRAR@UNIONGOV.COM; uge3125@uga.edu; vjohnson@lee.ga.us; votecw@elberton.net; voterreg@btconline.net; VOTERREGISTRAR@BULLOCHCOUNTY.NET; voterregistration@windstream.net; VOTETAYLOR@YAHOO.COM; VRMONTGOMERY@YAHOO.COM; warrenvotereg@classicsouth.net; wcboe.supervisor@gmail.com; wcprobate@classicsouth.net; WCREGISTRARS@WINDSTREAM.NET; WEBSTERFINANCE@WINDSTREAM.NET; weslewis@ccboc.com; WILCOX2115@WINDSTREAM.NET; wilkescovoter@hotmail.com; worthelechair@hotmail.com; WPROBATE@HOTMAIL.COM

Cc: Harvey, Chris; Broce, Candice; Rayburn, Kevin

Subject: Update from Homeland Security Regarding Election

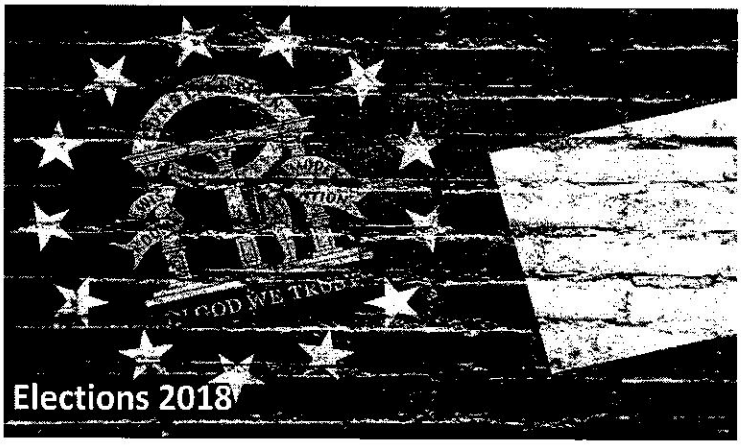
I just posted on Firefly under **Official Communications>Election Security General** a release from Department of

Homeland Security that highlights warning signs to be on the lookout for as we continue the preparations for early voting and Election Day, November 6, 2018.
This list, while extensive is not exhaustive.

Please make sure to review this notice and share this information with your election teams.

Chris Harvey
Elections Director, Georgia Secretary of State

404-657-5380 DIRECT
404-985-6351 MOBILE



Election Update

October 5, 2018

ELECTION COUNTDOWN: 32 DAYS TO GO

Columbus Day

October 8, 2018 is a state holiday (Columbus Day) and, as a result, the voter registration deadline will be October 9, 2018. The Secretary of State's Office is scheduled to be closed on Monday, October 8, 2018. We will have staff available should you need to reach us.

Election Security Information

The security of our elections should be one of your highest priorities. It is important to stay up-to-date on security concerns and best practices. We post election security information on firefly under Official Communications > Election Security General. We strongly encourage that you consider joining EI-ISAC https://www.cisecurity.org/ei-isac/. It is free to join and the Secretary of State's Office and several Georgia counties have already joined. EI-ISAC puts out weekly election security information and is a great resource for your election security toolkit.

Pending Age Voters

If a voter is 18 years of age by November 6, 2018, they can vote in the General Election. The system keeps the voter in Pending Age Status until they turn 18 years old. When processing absentee ballot requests, the birthday of the pending age voter needs to be checked and if it is November 6, 2018 or earlier, remove the challenge status in the Ballot Returned section of the absentee ballot screen and the ballot can then be issued. Pending Age voters are unique because of their status and they are eligible to vote a ballot that is not challenged unless there is another reason to challenge them.

VoteSafe

State law requires the voter lists be available to the public, including the names and addresses of registered voters. In 2009, the Georgia Legislature enacted House Bill 227, known as the VoteSafe program, to provide for the confidentiality of residence addresses of certain registered voters who have been, or may be, subject to acts of family violence, stalking, or currently reside in a family violence shelter. Once a VoteSafe application is approved for an elector, it is active for four years. To review the requirements for the VoteSafe program, please reference O.C.G.A. § 21-2-225.1(a).

The information provided in the Vote Safe application and accompanying documents are strictly confidential. Counties should develop a method of storing these materials that protects this confidentiality.

Upon acceptance, the voter will have VoteSafe status for four years or until the voter registration is transferred out of your county. At the end of four years, or upon moving out of the county, a voter would need to reapply to the program.

CHRIS HARVEY | ELECTIONS DIRECTOR | SECRETARY OF STATE'S OFFICE | (404) 656-2871

OFFICIAL ELECTION BULLETIN

October 17, 2018

TO: **County Election Officials and County Registrars**

FROM: **Chris Harvey, Elections Division Director**

RE: **Security, Poll Watchers, and Press During Voting**

Security is a high priority as the election looms and advance voting begins. As we have pointed out repeatedly, part of our election security is based on multiple layers of security including physical security of equipment and locations where equipment is stored or voting takes place.

I am again encouraging all election officials to remain vigilant throughout the period of advance voting and on Election Day. This includes high levels of awareness of all activities that take place within areas where voting occurs, and where voting equipment is stored.

Special attention must be paid to individuals seeking access to secure areas or voting equipment. If a person states that they are from a vendor, or the Secretary of State's Office, or that they have some official status, identification should be checked and verified further by telephone if necessary to establish a person's identity and authority.

Be aware that in the aftermath of an unusual event such as the Hurricane, some individuals or groups might attempt to take advantage of unusual situations to gain access to secure areas either physically or by electronic/cyber means. Phishing emails remain the greatest threat to cyber security. One of the best ways to protect yourself is to practice a slow and methodical approach to responding to emails, and to be hesitant to open attachments or links in emails, or to verify by telephone that an email is authentic if there is cause for alarm.

The Republican and Democratic parties and the Libertarian political body have appointed statewide poll watchers, and likely, many counties have poll watchers for local polling places. We have posted the list of the poll watchers on Firefly under the "2018 General Election Information" folder.

To specify some activities poll watchers may not engage in while behind the enclosed space:

1. In no way interfere with the conduct of the election;
2. May not talk to voters;
3. May not check elector lists;
4. May not use photographic or other electronic monitoring or recording devices;
5. May not use cellular phones;
6. May not participate in any campaigning;
7. May not compromise the privacy of the voter's secret ballot.

I encourage you to review O.C.G.A. 21-2-408(d) for the entire code regarding poll watchers and the poll manager's rights and responsibilities concerning poll watchers in a polling place:

"(d) Notwithstanding any other provisions of this chapter, a poll watcher may be permitted behind the enclosed space for the purpose of observing the conduct of the election and the counting and recording of votes. Such poll watcher shall in no way interfere with the conduct of the election, and ***the poll manager may make reasonable regulations to avoid such interference****. Without in any way limiting the authority of poll managers, poll watchers are prohibited from talking to voters, checking electors lists, using photographic or other electronic monitoring or recording devices, using cellular telephones, or participating in any form of campaigning while they are behind the enclosed space. If a poll watcher persists in interfering with the conduct of the election or in violating any of the provisions of this Code section after being duly warned by the poll manager or superintendent, he or she may be removed by such official. Any infraction or irregularities observed by poll watchers shall be reported directly to the superintendent, not to the poll manager. The superintendent shall furnish a badge to each poll watcher bearing the words "Official Poll Watcher," the name of the poll watcher, the primary or election in which the poll watcher shall serve, and either the precinct or tabulating center in which the poll watcher shall serve or a statement that such poll watcher is a state-wide poll watcher. The poll watcher shall wear such badge at all times while serving as a poll watcher."* (emphasis added)

Poll watchers must be monitored to ensure that they are not exceeding their authority, interfering with voting, infringing on voter privacy, or gaining access to any equipment or data which they have no authority to access.

There is also significant press interest in these elections, and I expect media requests for access to report from and/or photograph or record video in polling places to be plentiful. O.C.G.A. 21-2-413(e) specifies:

"(e) No person shall use photographic or other electronic monitoring or recording devices, cameras, or cellular telephones while such person is in a polling place while voting is taking place; provided, however, that a poll manager, in his or her discretion, may allow the use of photographic devices in the polling place under such conditions and limitations as the election superintendent finds appropriate, and provided, further, that no photography shall be allowed of a ballot or the face of a voting machine or DRE unit while an elector is voting such ballot or machine or DRE unit and no photography shall be allowed of an electors list, electronic electors list, or the use of an electors list or electronic electors list. This subsection shall not prohibit the use of photographic or other electronic monitoring or recording devices, cameras, or cellular telephones by poll officials for official purposes."

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
WASHINGTON, DC 20511

NCSC-18-502

MEMORANDUM FOR: The Honorable Christopher C. Krebs
Under Secretary for National Protection and Programs Directorate
Department of Homeland Security

The Honorable David J. Glawe
Under Secretary for Intelligence and Analysis
Department of Homeland Security

Mr. Joshua D. Skule
Executive Assistant Director, Intelligence Branch
Federal Bureau of Investigation

SUBJECT: **Election Security Information Needs**: Foreign Threats to U.S. Elections

The National Counterintelligence and Security Center (NCSC) is working closely with the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Election Assistance Commission, and other Federal agencies to assess and mitigate foreign governments' actions to interfere in U.S. elections. The Intelligence Community (IC) continuously reviews intelligence to identify foreign threats to the U.S. election infrastructure. The U.S. election infrastructure consists of (a) storage facilities, polling places, voter registration offices, and centralized vote tabulation locations used to support U.S. election processes, as well as (b) information and communications technology, including voter registration databases, voting machines, and other electronic systems used to manage U.S. election processes and display results on behalf of state and local governments. The national-level information needs we cite below are intended to be disseminated to election officials at all levels (state, local, tribal, and territorial) to help them identify, understand, report on and counter any efforts to interfere in U.S. elections. I encourage you to disseminate these information needs to election officials to the widest extent possible to encourage the reporting of suspected or confirmed threats to U.S. electoral infrastructure or election activities.

Foreign governments' efforts to interfere with U.S. elections fall into four distinct categories: (a) cyber operations targeting election infrastructure; (b) cyber operations targeting political organizations, campaigns, and public officials; (c) influence operations to assist or harm political organizations, campaigns, and public officials, or to sway public opinion and sow division; and (d) physical threats to polling places and election offices. Election officials are encouraged to report to DHS and FBI any indicators that foreign actors may be engaged in the following activities prior to, during, and following the day of the election, to include:

SUBJECT: **Election Security Information Needs**: Foreign Threats to U.S. Elections

1. Unauthorized entry or attempts to gain access to long term storage facilities, polling places, and voter centers, including those that may be located on public or private property, used to store election and voting system infrastructure.

2. Incidences of spear-phishing or attempts to hack voter registration systems, to include similar efforts against seemingly unrelated state or local government entities, such as the Department of Motor Vehicles or other agencies or civic organizations responsible for registering voters.

3. Attempts to access, alter, or destroy systems used to qualify candidates; produce and deliver ballots; procure, manage and prepare voting equipment; process requests for absentee ballots; and store and manage election administration process and procedure documentation.

4. Unauthorized access, or attempts to access, IT infrastructure or systems used to manage elections, including systems that count, audit, or display election results on election night and systems used to certify and validate post-election results.

5. Attempts to hack, spear-phish, or compromise personal or professional e-mail accounts and social media accounts of elections officials, staff and volunteers.

6. Hacking attempts or successful hacks into political party headquarters or candidate IT systems.

7. Attempts to access, hack, alter, or disrupt infrastructure to receive and process absentee ballots through tabulation centers, web portals, e-mail, or fax machines; attempts to interfere with votes sent through the U.S. Postal Service.

8. Compromises of any networks and/or systems, including hardware and/or software, by cyber actors to include the tactics, techniques, procedures and impact observed on election-related networks and systems; evidence of interference detected on state networks or systems for cyber security indicators of compromise.

9. Instances of any unexplained disruption at polling stations or training locations for voting officials, including early voting locations, which block or limit voter turnout. Disruptions may include social media posts or robocalls falsely reporting closed or changed polling stations, or physical incidents at polling stations, including distribution of false information.

10. Disinformation efforts to alter or shutdown government web sites to foment social unrest or reduce voter turnout, to include on social media or other electronic means.

11. Unauthorized entry of centralized vote counting/tallying locations or electronic systems or networks used by states and localities to count absentee/military and election day voting ballots.

SUBJECT: **Election Security Information Needs**: Foreign Threats to U.S. Elections

12. Impacts to critical infrastructure that limit access to polling stations such as power, water, internet, telephone (cellular), and transportation (traffic controls) outages.

William R. Evanina

9-5-18
Date

cc: see Distribution List

SUBJECT: **Election Security Information Needs**: Foreign Threats to U.S. Elections

Distribution:

Director of National Intelligence
Under Secretary of Defense for Intelligence
Director of Intelligence, J-2, Joint Chiefs of Staff
Director, Office of Intelligence and Counterintelligence, Department of Energy
Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security
Assistant Secretary of State for Intelligence and Research
Assistant Secretary of the Treasury for Intelligence and Analysis
Executive Assistant Director, Intelligence Branch, Federal Bureau of Investigation
Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, National Geospatial-Intelligence Agency
Director, National Reconnaissance Office
Director, National Security Agency
Chief of Intelligence/Senior Officer, Drug Enforcement Administration
Deputy Chief of Staff, G2, United States Army
Director of Intelligence, Headquarters, United States Marine Corps
Director of Naval Intelligence, United States Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, United States Air Force
Assistant Commandant for Intelligence and Criminal Investigations, United States Coast Guard

2 October 2018

(U) A Georgia Perspective on Threats to the 2018 U.S. Elections

(U) Prepared by the DHS Office of Intelligence & Analysis (DHS I&A), Field Operations Division, Southeast Region. Coordinated with the DHS I&A Cyber Mission Center.

(U//FOUO) ***DHS I&A assesses that foreign governments may engage in cyber operations targeting the election infrastructure and political organizations in Georgia and engage in influence operations that aim to interfere with the 2018 U.S Elections.*** The motives of these cyber actors and foreign influencers may vary; they may intend to disrupt political processes, sway public opinion, or to support or undermine certain political organizations. In the past month, DHS observed multiple tactics targeting election related infrastructure at the local and state level to include, but not limited to, spearphishing, Cross Site Scripting (XSS), Structured Query Language Injections (SQLI), and attempted Denial of Service (DoS) attacks.[1,2]

(U) DHS I&A is particularly concerned about the potential for the following activities related to the 2018 U.S. election:[1]

- (U) Unauthorized entry to polling places or long-term storage facilities, and voting facilities used to store election and voting system infrastructure.
- (U) Incidents of spearphishing or attempts to hack voter registration systems, such as Department of Motor Vehicles (DMV) or other organizations used to register voters.
- (U) Attempts to access information technology (IT) infrastructure used to manage elections, display results, or for counting or certifying votes.
- (U Hacking or spearphishing attempts against the emails or social media accounts of election officials, staff or volunteers.
- (U) Hacking attempts of political party headquarters or candidate's IT systems or websites.
- (U) Attempts to hack, alter or disrupt infrastructure used to process absentee ballots or attempts to interfere with votes sent through the US Postal Service.
- (U) Compromise of any networks or systems by cyber actors, including tactics, techniques, and procedures, along with the impact observed on election-related systems.
- (U) Any unexplained disruptions at polling places or training locations which block or limit voter turnout. This may include social medial messages or robo-calls falsely reporting changed or closed polling locations, or physical incidents at polling locations, including distribution of false information.
- (U) Disinformation efforts to shut down government websites to foment social unrest or reduce voter turnout.
- (U) Impacts to critical infrastructure that limit access to polling stations, such as power outages, internet, telephone (cellular), and transportation (traffic control) outages.[3]

(U) Election officials are encouraged to report any activity related to the above information needs to the Georgia Secretary of State's Office.

---

[1] For additional elections security related resources visit https://www.dhs.gov/publication/election-security-resources

[1] (U//FOUO) DHS; IIR 4 007 0590 18; (U//FOUO) Attempts to Illegally Access Online Voter Registration Database Using Structured Query Language Injections and Cross Site Scripting; Extracted Information is (U//FOUO); Overall document is (U//FOUO).
[2] (U//FOUO) DHS; IIR 4 007 0605 18; (U//FOUO) Spoofing of Senior State Election Official Email Address to Send Spearphishing Email to City Government Official; Extracted Information is (U//FOUO); Overall document is (U//FOUO).
[3] (U) ODNI Director of the National Counterintelligence and Security Center; NSCS-18-502; (U) Election Security Information Needs: Foreign Threats to U.S. Elections; 05 SEP 2018.